AUDITOR GENERAL

WILLIAM O. MONROE, CPA

FLORIDA STATE UNIVERSITY

CASHIERING SYSTEM

Information Technology Audit

SUMMARY

The Florida State University (University) Cashiering System supports the business processes for receipting, depositing, and recording the collection of University moneys. The primary user of the Cashiering System was the Office of Student Financial Services. Administrative Information Systems (AIS) provided programming support for the Cashiering System. Storage and processing resources were provided by Northwest Regional Data Center (NWRDC).

Our audit focused on management controls and selected information technology (IT) functions applicable to the Cashiering System during the period September 2002 through January 2003.

Certain deficiencies were noted in IT security and general management controls. Specifically, these deficiencies included:

Finding No. 1: Improvements were needed in the University's IT risk management practices.

Finding No. 2: Deficiencies were noted in the University's IT security controls.

BACKGROUND

The Cashiering System was implemented in 1987 to automate the receipting, depositing, disbursement, and recording of cashiering transactions for the University. The Office of Student Financial Services is under the direction of the University Controller's Office.

The Office of Technology Integration (OTI), which was comprised of AIS, Academic Computing and Network Services, User Services, and Information Resource Management, was responsible for providing IT resources to meet the needs of the University. AIS was responsible for providing business solutions and services to the University, including the provision of programming support for the Cashiering System. Storage and processing resources for the Cashiering System were provided by NWRDC.

Finding No. 1: IT Risk Management

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization, and its ability to perform its mission, from IT-related risk. The risk management process involves identifying and assessing risk, and taking steps to reduce risk to an acceptable level.

We noted deficiencies in the University's IT risk management practices. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising University information. However, the appropriate University personnel have been notified of the deficiencies.

Recommendation: The University should implement the appropriate IT risk management practices to provide increased assurance that IT-related risks are identified and managed in a cost-effective manner.

Finding No. 2: Security Control Deficiencies

Effective security relies on a security structure that includes operational procedures, organization, and resources. The University's IT security controls were deficient in the following areas:

- The University's position descriptions for OTI staff and OTI management with sensitive responsibilities did not, in many instances, designate these positions as positions of special trust requiring pre-employment background checks, although University policies and procedures required pre-employment background checks for sensitive positions or positions of special trust. Specifically, the University had not designated a requirement for background checks on position descriptions for OTI personnel engaged in certain IT duties, including those responsible for data security and the maintenance of sensitive and confidential data assets. Neither had background checks been conducted for these positions. However, we noted that the University had classified certain members of the Enterprise Resource Planning project and the new director of the NWRDC as positions of special trust on their position descriptions and had accordingly conducted background checks on these individuals. Background security checks on designated IT personnel enhance security within the IT environment and may mitigate certain legal actions against the University should such an employee commit an unauthorized action.

- The University did not maintain complete security administration procedures. Documentation of security administration functions provides the security administrator with specific steps to administer and monitor security functions to match University policy. These documents should provide IT management with a guide to ensure effective performance of security practices by backups or new employees assigned to security administration positions. The University had not developed comprehensive procedures over the security administration functions, including formally defining the University's security configuration. Such documentation should include specific access control methodologies for administering user logon identification structures, auditing controls, and customized controls employed. Although the University maintained a high-level document for the security management of the mainframe, the Cashiering System, and database security administration, this document did not provide formal procedures for granting access to other system functions including security measures for application programmers. Also, the document did not include detail on customized scripts deployed to provide special controls that may not have been part of the standard functions of the different security applications. Additionally, documentation was not maintained for security administration function duties for administrators of network equipment (such as switches and routers). Functionally, rather than relying on formal security administration procedures, each area of security administration relied on University policies, informal procedures, and institutional knowledge of the respective security administrator to maintain system security.

- We noted other deficiencies in certain security control features implemented by the University. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising the University's information. However, appropriate University personnel have been notified of these deficiencies.

Given the deficiencies noted above, there is an increased risk that the integrity, confidentiality, and availability of University data and IT resources could be compromised and not timely detected.

Recommendation: The University should implement stronger security features in the areas noted above.

OTHER MATTERS

The Health Insurance Portability and Accountability Act of 1996[1] (HIPAA) addresses data interchange, privacy, and information security standards for personal health information. Pursuant to HIPAA, the United States Department of Health and Human

[1] Public Law 104-191

Services has published regulations on electronic data interchange standards, privacy, and security. The final Transaction Rule, which contains electronic data interchange standards, was incorporated as a Federal regulation and had a compliance date of October 16, 2002. The final Privacy Rule was incorporated as a Federal regulation and compliance was required by April 14, 2003. The final Security Rule was incorporated as a Federal regulation and has a compliance date of April 21, 2005. HIPAA also provides for civil and criminal penalties for noncompliance. The University had determined that the Thagard Student Health Center (Health Center) falls under current provisions of HIPAA. The Health Center instituted policies, procedures, and other security measures relating to specific provisions of the Act. The University should continue to evaluate the impact of HIPAA requirements on all University IT activities due to the dynamic nature of the data transmitted over the network by University units which may be subject to this Act in the future.

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this audit focused on evaluating selected IT functions applicable to the Cashiering System during the period September 2002 through January 2003. Our objectives were to determine the effectiveness of selected IT controls related to the Cashiering System.

To meet our audit objectives, we reviewed applicable Florida Statutes, administrative rules, and auditing literature; interviewed appropriate University personnel; obtained an understanding of management controls relating to selected IT functions; observed control processes and procedures; and performed various other audit procedures to test selected controls related to the Cashiering System.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

AUDITEE RESPONSE

In a response letter dated December 24, 2003, the University generally concurred with our audit findings and recommendations. The University's response can be viewed in its entirety on the Auditor General Web site.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Brian Rue, CPA*, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.state.fl.us/audgen); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

The Florida State University
Office of Audit Services
Suite 407 Westcott Building
Tallahassee, Florida 32306-1390

December 24, 2003

Mr. William O. Monroe, CPA
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Subject: Information Technology Audit of the Florida State University Cashiering System, for the period September 2002 through January 2003, dated December 9, 2003.

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, the University's written statement of explanation concerning all of the preliminary and tentative findings, including our actual or proposed corrective actions, is enclosed.

Should you have any questions, or desire additional information, please let me know. Thank you.

Cordially yours,

David P. Coury
Chief Audit Officer

cc: John Carnaghi
Joe Lazor
T. K. Wetherell

Enclosure

Written statement of explanation – preliminary and tentative findings, including actual or proposed corrective actions.

Information Technology Audit of the Florida State University Cashiering System, for the period September 2002 through January 2003, dated December 9, 2003.

Finding No. 1: Improvements were needed in the University's IT risk management practices.

Recommendation: The University should implement the appropriate IT risk management practices to provide increased assurance that IT- related risks are identified and managed in a cost-effective manner.

We concur that an effective risk management process is an important component of a successful IT security program. Our Information Technology Security Policy, Information Technology Security Plan, related IT policies and procedures, as well as our security awareness and training sessions, serve as the foundation of our overall information technology security strategy.

Most notable, the University has completed an enterprise level, risk analysis of the campus network, application, and users layers. We have also formed a campus wide information technology risk analysis team that will be responsible for developing and coordinating college, school, and departmental level risk analysis on a recurring basis. The team is working to validate previously identified risks with accompanying corrective actions needed to reduce or eliminate those risks to the campus information technology infrastructure. The projected completion date for that effort is April 30, 2004.

Finding No. 2: Deficiencies were noted in the University's IT Security Controls

Recommendation: The University should implement stronger security features in the identification of positions of special trust, related background checks, and security documentation for system administrators.

We concur. The Office of Technology Integration is already working with all parties to identify related positions of special trust, revise position descriptions to reflect that "special trust", require successful completion of background checks as a condition of employment. The projected completion date for this effort is March 24, 2004.

A security system administrator manual for ACF2, and FSEC is being finalized to supplement existing security documentation for system administrators. The projected completion date for that effort is February 25, 2004.